IN THE CLAIMS

1. (Previously Presented) A computer-implemented method for computer virus prevention, said method comprising the steps of:

entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network;

computing a first computer virus alert time corresponding to entry into the first computer virus status mode;

comparing a time stamp of executable computer code corresponding to an earliest moment the computer code was allowed to execute on a computer coupled to the computer network with the first computer virus alert time; and

determining the executability of the computer code in response to the result of the comparing step.

2. (Original) The method of claim 1, wherein the step of computing the first virus alert time comprises the steps of:

receiving a first access control time based on the first virus outbreak report; and

converting the first access control time into the first virus alert time.

3. (Original) The method of claim 2, wherein the first access control time is a relative time stamp.

4. (Original) The method of claim 2, wherein the first access control time is a pre-determined time period for access control under the first computer virus status mode.

5. (Previously presented) The method of claim 1, further comprising the step of:

determining the presence of a value representing the computer code in a memory table of executable computer content.

6. (Previously presented) The method of claim 5, wherein the computer code is not executed when the value representing the computer code is not present in the memory table of executable computer code.

7. (Previously presented) The method of claim 5, wherein the value is a hash value of the computer code.

8. (Previously presented) The method of claim 1, wherein the computer code is determined to be executable only when the computer code is time stamped prior to the first computer virus alert time.

9. (Original) The method of claim 1, further comprising the steps of:

entering types of computer codes that should be blocked from execution in response to the first computer virus outbreak report; and

blocking execution of a computer code that belongs to the entered types of computer codes.

10. (Previously presented) The method of claim 1, further comprising the steps of:

generating a second virus alert time in response to a second computer virus outbreak report;

comparing the time stamp of the computer code with the second computer virus alert time;

performing anti-virus processing upon the computer code; and

determining the executability of the computer code in response to the result of comparing the time stamp of the computer code with the second computer virus alert time.

11. (Previously presented) The method of claim 1, wherein the computer code is attached to an E-mail body, and said method further comprises the steps of:

removing the computer code from the E-mail body; and

denying execution of the computer code.

12. (Previously Presented) A computer access control system for computer virus prevention, said system comprising:

a computer configured to execute an access control console, for entering a first computer virus status mode in response to receiving a computer virus outbreak report indicating a virus attack threat to a computer network and for recovering a preselected virus access control time corresponding to said virus status mode; and

an anti-virus module, coupled to the access control console, configured to compute a virus alert time based on the virus access control time and to compare a time stamp of target executable computer code corresponding to an earliest moment the computer code was allowed to execute on a computer coupled to the computer network with the virus alert time prior to execution of the target executable computer code, and

wherein the anti-virus module is further configured to determine whether to execute the target executable computer code in response to comparing the time stamp of the target executable computer code with the virus alert time.

13. (Previously presented) The system of claim 12, wherein the target computer code is one of a plurality of computer code files, and the anti-virus module further comprises:

a memory module for storing time stamps of the plurality of computer code files; and

an access control module, coupled to the access control console and to the memory module, for computing the virus alert time and for comparing the time stamp of a target executable computer code with the virus alert time.

14. (Previously presented) The system of claim 13, wherein the anti-virus module further comprises:

a computer virus processing module, coupled to the access control module, for further processing the target executable computer code in order to determine whether to execute the target executable computer code.

15. (Previously presented) The system of claim 13, wherein the memory module stores a value representing each of the computer code files.

16. (Previously presented) The system of claim 15, wherein the access control module is configured to determine the presence of the value in the memory module as representing a target executable computer code.

17. (Original) The system of claim 15, wherein the value is a hash value.

18. (Canceled)

19. (Canceled)

20. (Previously Presented) A computer-implemented method for computer virus prevention, said method comprising the steps of:

creating a list of executable computer files, each file time-stamped with an execution time of the file, the execution time corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to a computer network;

entering a virus alert mode in response to a virus outbreak report indicating a virus attack threat to the computer network;

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking the execution of suspicious or susceptible executable computer files that have a time stamp not before a computed virus alert time, the access control message including a first control parameter for computing the virus alert time;

receiving a request to execute a target executable computer file; and

determining whether to execute the target executable computer file based on the access control rule in the access control message.

21. (Canceled)

22. (Previously presented) The method of claim 20, wherein the step of determining whether to execute the target computer file comprises the steps of:

receiving the access control message;

automatically converting the first control parameter into the virus alert time;

comparing the time stamp of the target computer file in the list with the virus alert time; and

determining whether to execute the target executable computer file based on the result of the comparing step.

23. (Previously presented) The method of claim 22, further comprising the step of:

applying an anti-virus operation upon the target executable computer file.

24. (Previously presented) The method of claim 20, wherein the control message comprises:

a second control parameter for specifying types of computer files that should be subject to the access control rule;

a third control parameter for specifying an expiration time for the access control rule; and

a fourth control parameter for identifying the access control message.

25. (Original) The method of claim 24, further comprising the step of:

determining validity of the access control message based on the third control parameter.

26. (Previously presented) The method of claim 24, further comprising the step of:

determining whether to execute the target executable computer file based on the second control parameter.

27. (Previously Presented) A computer-implemented method for computer virus prevention, said method comprising the steps of:

creating a list of executable computer files, each file time-stamped with an execution time of the file;

entering a virus alert mode in response to a virus outbreak report indicating a virus attack threat to a computer network;

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking data communication initiated by computer files that have a time stamp corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network, and the time-stamp is not before a virus alert time, the access control message including a first control parameter for computing the virus alert time;

receiving a request to examine a target executable computer file that participates in the data communication; and

determining whether the data communication should be blocked based on the access control rule.

28. (Previously presented) The method of claim 27, wherein the step of determining whether the data communication should be blocked comprises the steps of:

receiving the access control message;

converting the first control parameter into the virus alert time;

comparing the time stamp of the target executable computer file in the list with the virus alert time; and

determining whether the data communication should be blocked based on the comparing step.

29. (Previously presented) The method of claim 28, wherein the data communication is blocked when the target executable computer file is time-stamped not before the virus alert time.

30. (Previously Presented) A computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

a firewall module monitoring data communications initiated by a target executable computer file and sending a request to examine the data communications;

an access control console, for generating an access control message specifying an access control rule for blocking data communications of the target executable computer file that has a time stamp corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to a computer network, and the time-stamp is not before a virus alert time, the access control message including a first control parameter for computing the virus alert time in response to receiving a virus outbreak report indicating a virus attack threat to the computer network; and

an access control module, coupled to the access control console and the firewall module, configured to receive the access control message and a request from the firewall module, and to compute the virus alert time based on the virus access control time and to determine whether the data communication should be blocked based on the access control rule.

31. (Previously Presented) A computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

a computer readable program code device configured to receive a computer virus status mode in response to a computer virus outbreak report indicating a virus attack threat to a computer network;

a computer readable program code device configured to compute a computer virus alert time corresponding to entry into the computer virus status mode;

a computer readable program code device configured to compare a time stamp of an executable computer file corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network with the computer virus alert time; and

a computer readable program code device configured to determine whether to execute the executable computer file in response to the result of comparing the time stamp of the computer content with the computer virus alert time.

32. (Previously Presented) A computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

means for entering a computer virus status mode in response to receiving a virus outbreak report indicating a virus attack threat to a computer network and for generating a virus access control time;

coupled to the entering and generating means, means for computing a virus alert time based on the virus access control time; and

coupled to the computing virus alert time means, means for comparing a time stamp of a target executable computer file corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network with the virus alert time prior to execution of the target executable computer file and for determining whether to execute the target executable computer file in response to comparing the time stamp of the target executable computer file with the virus alert time.

33. Canceled.

34. (New) A computer-implemented method for computer virus prevention, said method comprising the steps of:

entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network;

computing a first computer virus alert time corresponding to entry into the first computer virus status mode;

comparing a time stamp of executable computer code corresponding to a first time the computer code was allowed to execute on a computer coupled to the computer network with the first computer virus alert time; and

determining the executability of the computer code in response to the result of the comparing step.